Problem Resolution Report

CoSD Contract no. 537863
Mobile Device Management - AirWatch
HP/CoSD-123

Date: March 4, 2014

Summary

In accordance with the provisions of the IT and Telecommunications Service Agreement by and between the County of San Diego ("County") and HP Enterprise Services, LLC ("HP" or "Contractor" and hereinafter collectively referred to as "the Parties") originally dated January 24, 2006 and restated on April 5, 2012 ("the Agreement"), agreement is reached on the Effective Date shown below.

Issue or Problem:

The County's mobility strategy calls for the increasing business use of smart phones and media tablets. Many of these devices are currently managed by a legacy Mobile Device Management service. While this system has been successful in supporting a number of mobile machines, it does not support popular platforms such as Android based devices.

Resolution:

1. The Mobile Device Management Resource Unit is intended to allow faster and lower-cost adoption of productivity-enhancing iPhones, iPads, Windows phone/tablets and Androids; central control of corporate data (without impacting personal data); and enhanced security compliance across the enterprise. It enables the Contractor to manage, control and report on all mobile devices and platforms.

2. The Contractor shall provide Centralized, secure Mobile Device Management services for iOS, Android and Windows Phone 7 devices (smart phones or media tablets). With the Blackberry platform currently in place, the Parties agree to exclude it from this solution and continue to manage it as-is.

3. The monthly Resource Unit Fees are assessed per device with the rate dependent upon the total number of devices managed under this Resource Unit with a minimum of 1,000 devices enrolled. The Resource Units Fees are as follows:

Total Quantity of Mobile Devices	Monthly Fee
≤ 1000	$ 9,330
1001 - 1499	$ 9.33 per device
1500 - 1999	$ 6.73 per device
≥ 2000	$ 5.93 per device

The first 90 calendar days of system deployment or once 1,000 devices are enrolled shall be defined as the "Ramp Up Period". The trigger for the start of the Ramp Up Period shall be the jointly agreed upon certification that the Airwatch platform is installed, tested and ready to accept users. At that point, all devices currently enrolled in the current Device Management Service ("Legacy MDM"), including ActiveSync devices will be transferred into the new Airwatch Mobile Device Management environment on an expedited basis.

During this Ramp Up Period a $9.33 per-device fee will be charged for any enrolled device, regardless of the actual volume. At the expiration of the Ramp Up Period or until 1,000 devices are enrolled (whichever comes first), the applicable Resource Unit Fees will become effective.

During the Ramp Up Period all the devices still under the Legacy MDM and not yet transitioned, will be subject to the existing Mobile Devices Management Services Resource Unit.

4. The baseline volume for this Resource Unit is 2,000 enrolled devices/month.

5. Once the baseline volume of 2,000 mobile devices is reached, an additional License Fee in the amount of $47.50 will be charged for any net device in excess of 2,000. License True-up will be conducted quarterly beginning the calendar quarter following the County exceeding the baseline volume

6. The above pricing is based on the one time expenditure of the portion of funds required to support this PRR from the End Switch Reinvestment Credit established in PRR 083 in the amount of $151,000.

7. The following services are not included in the Mobile Device Management services:

- Deployment of device operating systems and firmware updates;
- Hardware support for devices or resolution of provider service issues for devices

8. Costs for the EIS Cloud Connector servers (one for each data center) and for data storage are not included in this Resource Unit. These costs are covered under the appropriate server and storage RUs .

9. Approval of this PRR and implementation of this new solution is intended to be complete replacement for the existing MDM platform, including devices in ActiveSync. The parties agree that all users of the legacy MDM platform will migrate to Airwatch system within 60 days
10. Section 4.11- Mobile Device Management in Schedule 4.3 – Operation Services of the Agreement is hereby replaced in its entirety as per Attachment 1 to this PRR 123.

11. Section 22 – Mobile Device Management Services of Schedule 16.1 – Fee, is hereby replaced in its entirety as per Attachment 2 to this PRR 123;

12. Schedule 16.1-5 is hereby revised to reflect the new Mobile Device Management Resource Unit Fees, as shown in Attachment 3 to the PRR 123.

****

Attachment 1 to PRR 123 – Mobile Device Management - AirWatch

4.11 Mobile Device Management

4.11.1 Mobile Device Management Services Overview

This section pertains to the Mobile Device Management (MDM) Services component within the Desktop Services Framework. The Mobile Device Management Services are intended to allow faster and lower-cost adoption of productivity-enhancing iPhones, iPads Windows Phones/Tablets and Android devices; central control of County data (without impacting personal data); and enhanced security compliance across the enterprise. These services enable the Contractor to centrally manage and control all mobile devices, platforms and applications from a single unified console.

4.11.2 Mobile Device Management High Level Requirements

4.11.2.1 Contractor shall provide centralized, secure Mobile Device Management services for iOS, Android and Windows Phone devices (smart phones or media tablets).

4.11.2.2 Mobile Device Management Services shall include:

- Over-the-air (OTA) self-provisioning, policy setting on device and connection configuration, including the ability to set encryption, ActiveSync, VPN configuration and WiFi settings with audit verification to streamline activations and eliminate the need for IT involvement.

- All device policies will be based on County security and data policies developed into MDM platform format and recommended by the Contractor and approved by the County.

- Management and support of mobile devices management application includes MDM application updates, point releases and fixes as required; perform routine database maintenance, policy maintenance and backups; maintain the MDM configuration; troubleshoot MDM service-related issues; maintain certificates and password resets as required.

- Security enforcement to continuously audit all connected devices and quarantine or revoke service for unmanaged or compromised devices.

- Security protection to maintain control of County information and selectively wipe only County data and applications, or all data, from managed devices with audit of successful completion.

- Simplification of mobile application deployment with an enterprise-specific OTA catalog of mandatory, recommended and available

Problem Resolution Report

CoSD Contract no. 537863
Mobile Device Management - AirWatch
HP/CoSD-123

The resolution of the issue or Problem as described in this Problem Resolution Report shall govern the Parties' actions under the Agreement until a formal amendment of the Agreement is implemented in accordance with the terms of the Agreement, at which time this Problem Resolution Report shall be deemed superseded and shall be null and void.

All other terms and conditions of the Agreement remain unchanged and the Parties agree that such terms and conditions set forth in the Agreement shall continue to apply. Unless otherwise indicated, the terms used herein shall have the same meaning as those given in the Agreement.

IN WITNESS WHEREOF, The Parties hereto, intending to be legally bound, have executed by their authorized representatives and delivered this Problem Resolution Report as of the date first written above.

COUNTY OF SAN DIEGO		**HP ENTERPRISE SERVICES, LLC**	
By:	John M. Pellegrino	By:	
Name:	JOHN M. PELLEGRINO	Name:	Max Pinna
Title:	Director Department of Purchasing and Contracting	Title:	Contracts Manager
Date:	3-5-14	Date:	March 4, 2014

HUDSON

applications, without requiring the use of a commercial Application Store such as GooglePlay or iTunes Store.

4.11.3 Mobile Device Management Services Scope of the Environment

4.11.3.1 Supported Devices

The mobile devices supported on this service must be capable of being managed by the solution in place, which has been approved by the County/Contractor joint Enterprise Architecture Team. The devices must also meet the following minimum requirements:

- Devices must operate on these operating systems:
  - iOS: OS version 4.x or later
  - Android: OS version 2.6 or later
  - Windows 7: OS version 7.10 or later

4.11.3.2 "Bring Your Own Device" Program

The "Bring Your Own Device" or "BYOD" program allows County employees to enroll personal mobile devices under the Mobile Devices Management Service. County policy will dictate when "BYOD" is allowed. Devices under a BYOD program must comply with the requirements listed in Section 4.11.3.1 above.

4.11.3.3 Devices excluded from the Mobile Devices Management Services

The following devices cannot be enrolled under the Mobile Devices Management Services:

- Devices that do not meet the criteria listed in Section 4.11.3.1 above
- Devices not authorized under the "Bring Your Own Device" Program
- Devices from County partners (such as Sheriff, DA, SDCERA)

4.11.4 Mobile Device Management Services Roles and Responsibilities

4.11.4.1 Authorize and Manage Mobile Users

Contractor shall manage mobile users by Active Directory (AD) group membership. This group membership will control end user's ability to enroll in the Mobile Device Management service.

4.11.4.2 Device Security Management

Contractor shall provide security management, including the general functionality described in this Resource Unit. The specific settings are defined by County policy as:

- Require passcode
- Wipe device after too many passcode attempts
- Restrict/Permit applications
- Restrict/Permit content
- Enforce application blacklist/whitelist
- Manage device configurations
- Manage Exchange and Active sync email configurations
- Ability to manage application sets and tie them to Active Directory is provided, but the labor for the addition, removal, modification or other actions for applications is not covered in this resource unit.
- In the event of lost or stolen assets, the asset will be wiped of all County data.

4.11.4.4 Mobile Device Application Store

An Enterprise Mobile Device Application store shall be provided. It can be used for application publishing to devices, through a push by user group. Labor for the creation or modification of applications for the Application Store shall be provided through Application Work Requests.

The Application Store can be accessed from all supported devices.

4.11.5 Mobile Device Management - Requirements, Roles and Responsibilities

The following table identifies the Plan Build and Operate requirements, roles and responsibilities associated with Mobile Device Management.

Mobile Device Management Services: Plan, Build and Operate Requirements Roles and Responsibilities		
Plan Requirements, Roles and Responsibilities	**Contractor**	**County**
1. Produce and submit Mobile Device Management solutions that best meet County business needs, security policies and service–level requirements	X	
2. Review and approve Mobile Device Management solutions		X
3. Perform and submit operational planning for Mobile Device Management capacity and performance purposes	X	
4. Review and approve operational planning for Mobile Device Management capacity and performance purposes		X
5. Design operational views and status for Ops Dashboard	X	
6. Review and approve operational views and statuses		X
7. Design operational reports per County Request	X	
8. Review and approve operational reports		X
9. Produce and submit Mobile Device Management operational policies and procedures including escalation	X	
10. Review and approve Mobile Device Management operational policies and procedures		X
Build Requirements, Roles and Responsibilities	**Contractor**	**County**
11. Develop and improve Mobile Device Management build as appropriate to improve performance	X	
12. Provide all test services and produce documentation required to support Mobile Device Management	X	
13. Produce and submit all test documentation to County	X	
14. Review and approve all test documentation		X
15. Provide all deployment services required to support Mobile Device Management	X	
16. Produce and submit to County all Mobile Device Management deployment documentation	X	
17. Review and approve all Mobile Device Management deployment documentation		X
18. Produce and submit plans to apply Mobile Device Management application releases and patches as required	X	
19. Review and approve Mobile Device Management application releases and patches plans		X
Operate Requirements, Roles and Responsibilities	**Contractor**	**County**
20. Manage all trouble tickets and services requests from inception to closure (e.g. recording, troubleshooting, escalating, coordinating, reporting, closing)	X	
21. Produce and submit end user instructions on provisioning and configuration of mobile devices	X	

22. Review and approve end user instructions on provisioning and configuration of mobile devices		X
23. Provide over-the-air (OTA) self-provisioning and connection configuration	X	
24. Perform routine database maintenance and backups to maintain optimal performance of the Mobile Device Management Platform	X	
25. Maintain the Mobile Device Management Platform configuration per engineering build documents and County policy	X	
26. Maintain all Mobile Device Management certificates for the platform and the devices	X	
27. Perform all device specified services through the Mobile Device Management console (e.g. remote wipes and password resets)	X	
28.Provide continuous monitoring of all connected devices for security issues	X	
29. Quarantine or revoke service for any unmanaged or compromised mobile device	X	
30. Manage mobile devices through Active Directory group membership	X	
31. Manage County approved BYOD devices to specific applications authorized by the County	X	
32.Utilize Ops Dashboard to monitor system performance	X	
33.Provide operational reports as requested	X	
34.Manage Enterprise Application Store to add and delete mobile applications	X	

Attachment 2 to PRR 123 – Mobile Device Management - AirWatch

Schedule 16.1.1 – Fees

22. Mobile Device Management Services (Reference Schedule 4.3 – Section 4.11)

This section pertains to the Mobile Device Management Services component within the Desktop Services Framework

22.1 Monthly Service Fees

Monthly Service covered under this section will be billed through the MDM Resource Unit including both County provided and Bring Your Own Device (BYOD) mobile assets.

22.~~1~~2 License Fee

An AirWatch License Fee in the amount of $47.50 fee shall be charged for each additional device in excess of 2,000.

Such charges shall be submitted quarterly and will be based on the net number of new devices added in the previous three-month period.

The County may choose to use available reinvestment funds established under PRR-083 for the quarterly license true-up.

ATTACHMENT 3 TO PRR 123 - MDM Airwatch

Resource Unit	Schedule 4.3 Cross-Reference/Service Framework Component **	Unit of Measure	Pricing	Resource Unit Fee (90% to 110% band)	Baseline Volumes (per Contract Year)	(Resource Unit Fee) x (Baseline Volume)	Bundled Resource Unit	Resource Unit Fee (70% to 80% band)	Resource Unit Fee (80% to 90% band)	Resource Unit Fee (110% to 120% band)	Resource Unit Fee (120% to130% band)	Resource Unit Fee (130% to150% band)	Resource Unit Fee (150% to200% band)	Measurement Methodology (Specific measurement on last day of month or cumulative use during month)	Depreciation Time Period (in Years)
Mobile Devices Management Services - **AirWatch** (Note: Standard banding does not apply. Specific pricing per volume as described)	Desktop Services - Mobile Devices Management Services--Section 4.11	Device	Fixed monthly fee per unit	$5.93 (2000+)	2,000	11,860	N/A	$9,330/month (1-1000)	$9.33/unit (1001-1499)	$6.73/unit (1500-1999)	$5.93/unit (≥ 2000)			**Specific**	N/A
Mobile Devices Management Services - **AirWatch** - License Fee	Desktop Services - Mobile Devices Management Services--Section 4.11	License	**Per License**	$47.50	N/A	N/A	N/A	N/A	N/A	N/A	N/A			**Specific**	N/A